

氏 名	川島 潤
授与した学位	博士
専攻分野の名称	工学
学位授与番号	博甲第3631号
学位授与の日付	平成20年 3月25日
学位授与の要件	自然科学研究科産業創成工学専攻 (学位規則第5条第1項該当)
学位論文の題目	組込みLinuxの高信頼化に関する研究
論文審査委員	教授 船曳 信生    教授 森川 良孝    教授 杉山 裕二

### 学位論文内容の要旨

近年、デジタル家電や携帯電話などの小型コンピュータが内蔵された組込み機器では、ネットワークを介した機器間の通信機能、動画や音声を再生するためのマルチメディア機能など、高度で複雑な処理が求められている。その要求を満たすため、ネットワークやマルチメディア機能に実績のある組込みLinuxをOSとして採用した製品が普及し始めている。組込みLinuxとは、様々なプロセッサやアーキテクチャを有する組込み機器に適用されたLinuxを指し、リアルタイム性、低リソース消費などの特徴を持つ。日常生活に密接に関係する組込み機器では、使用者の安全を守るために高い信頼性が要求されるため、組込みLinuxにおいてその高信頼性が重要な課題となっている。

サーバから組込み機器まで、様々な規模の計算機で動作可能なLinuxには、既に開発の終了した2.4と現在も開発が継続中である2.6の2つのバージョンが存在する。Linux 2.4は安定性に優れているため、セキュリティアップデートの機会が少ない組込み機器に適している。一方Linux 2.6は、スケーラビリティの高さから高性能なサーバに適している。また、携帯電話などの高性能な組込み機器ではLinux 2.6を基にした組込みLinuxが用いられている。組込みLinuxにおける高信頼化の課題として、2.4ではファイル暗号化・復号に加えプロセスアクセス制限も行うファイルアクセス制御機能の実装、2.6では安全な開発環境を提供する仮想化の実現が挙げられる。その際、低性能なプロセッサを利用した組込み機器上でも動作可能とする必要がある。

そこで本研究では、組込みLinuxの高信頼化の実現を目的として、ファイルアクセス制御機能とOSレベル仮想化機能の提案・実装・評価を行う。

まずLinux 2.4上のファイルアクセス制御機能として、セキュアファイルシステムSAS (Storage Add-on Security) を提案する。SASでは「プログラム中でオープンされたファイルオブジェクトはプログラム実行(execシステムコール)時に継承される」というLinuxの標準規約を利用することでOSの変更は不要としている。また、継承を用いてプロセスアクセス制限に利用する認証情報をアプリケーションに付与するため、認証情報を埋め込むといったアプリケーションの変更も不要としている。次にLinux 2.6上の仮想化技術として、組込みLinuxであるuClinux上でも動作するOSレベル仮想化システムuClinux-VServerを提案する。uClinux-VServerでは、Linuxが提供する資源管理フレームワークcgroupをOSレベル仮想化機能として利用することで、OSへの変更点を最小限としている。

本研究で実装したSASとuClinux-VServerの性能評価の結果、目的とする機能が実用上問題のない速度で動作することを確認した。今後の課題として、現在も機能拡張が行われているLinuxの資源管理フレームワークcgroupの変化に追従して、提案するuClinux-VServerを修正することが挙げられる。

## 論文審査結果の要旨

本論文では、組込み機器向けのOSとして、近年、その利用が広まっている組込みLinuxの高信頼化に関する2つの研究成果を報告している。Linuxは、オープンソースソフトウェアとして、世界中のソフトウェアエンジニアによって、その開発が進められており、仕様の公開性、機能の多様性、導入コストなどの面から非常に注目されている。

本論文では、組込みLinuxの高信頼化技術として、具体的には、ファイルアクセス制御のためのセキュアファイルシステムSAS、組込み機器上でのセキュアなソフトウェア開発環境のためのOSレベル仮想化機能uClinux-VServerを提案・実装している。セキュアファイルシステムでは、提案システムをカーネルモジュールとして実装することで、OSカーネルの変更不要、および、ファイルメタデータの暗号化を実現している。また、認証プログラムとプロセス間継承に関するLinuxでの標準規約を用いることで、特定のアプリケーションプログラムのみが本システムを利用可能としている。OSレベル仮想化機能では、OSレベル仮想化技術であるVServerと資源フレームワークcgroupを用いることで、提案システムが低性能の組込み機器上で動作すること、そのためのOSカーネル修正量を最小とすることを実現している。また、組込み機器に利用される、メモリ管理機構MMUを持たない低性能プロセッサ向けのOSであるuClinuxでも、提案システムの利用が可能となるように、主としてメモリ管理に関する修正も行っている。それぞれのシステムにおいて、ベンチマークテストを通じて実装システムの性能評価を行い、実用性を示している。

本論文のいずれの提案においても、Linuxカーネルやその関連ソフトウェア技術を駆使することで、他の類似システムにはない特徴を有する組込みLinux高信頼化のためのシステムを実現しており、その成果は、学位（工学）に値すると判断する。